US-PAT-NO: 4900904
DOCUMENT-IDENTIFIER: US 4900904 A
TITLE: Automated transaction system with insertable cards for downloading rate or program data
DATE-ISSUED: February 13, 1990
INVENTOR-INFORMATION:

NAME	CITY	STATE
Wright; Christopher B.	San Francisco	CA
Bristow; Stephen	Los Altos Hills	CA

US-CL-CURRENT: 235/381, 235/380 , 235/441 , 705/407 , 705/410

ABSTRACT: An automated transaction system employs portable rate cards having embedded memories for storing rate information corresponding to different services, and a terminal which receives an inserted rate card and operates to calculate the value of an item requested at the terminal by a user using the information stored in the rate card, and to dispense the requested item having the calculated value. In the preferred system, the rate cards are used for different postal carriers or different services of one carrier, and the item dispensed is a printed postmark corresponding to the value calculated and the selected carrier or service. The system also employs portable program cards which store programs for generating waybill forms used by different postal carriers or different postal services. The waybill generating program of a program card inserted in the terminal controls the display of the corresponding waybill form on the terminal display and the input of information to be printed on the resulting waybill.
20 Claims, 14 Drawing figures
Exemplary Claim Number: 1
Number of Drawing Sheets: 11

---------- KWIC --------

Brief Summary Text - BSTX (2): The invention relates to an automated transaction system which receives with a user card having a microprocessor for executing secure transactions in which an article or item of value is dispensed from a terminal, and an account balance stored in the card's memory is debited. In particular, the invention is applied to a postage transaction system in which a postage account is maintained within the microprocessor card and is used in transactions with postage printing and metering terminals.

Brief Summary Text - BSTX (4): Point-of-sale (POS) terminals and automated teller machines (ATM) have been widely used in conjunction with various types of cards issued to users for sale or credit transactions. For example, banks regularly issue account cards which have a magnetically coded number stored on a stripe for accessing the user's account through ATM terminals. Credit cards which have coded magnetic stripes are inserted in ATM or POS terminals to access a central account system for authorization of a credit transaction. There also have been proposals to use cards which

have large non-volatile memories, e.g. magnetic, integrated circuit (IC), or optical memory storage, for storing and retrieving information specific to the user, such as a medical history, biographical history, maintenance of an account balance and transaction history, etc.

Brief Summary Text - BSTX (5): These conventional systems generally employ a card which has a passive memory that is read in a card reader of computerized terminal maintained by a vendor. The security of the cards is problematic since most account cards used conventionally are passive and do not authenticate themselves or the particular transactions for which they are used. Instead, on-line access through a terminal to a central account system, such as bank or credit card account records, is required for confirmation of each transaction. This requirement places an access time and cost burden on vendors, such as bank branches and retail stores, which must maintain the terminal facilities, as well as on the operator of the central account system, which must provide sufficient on-line access for all the users of the system and ensure the security of the entire system.

Brief Summary Text - BSTX (6): By comparison, off-line transactions, i.e. between a user with an authorized card and a terminal not connected to a central account system, have the advantage that the vendor does not have to confirm each transaction. A card bearer merely inserts the card in a terminal to pay for a purchase and the authorized amount of the card is debited for the amount of the transaction. In off-line transactions, the vendor's responsibility can be reduced and the transaction process simplified, so that a transaction can be completely automated through the use of widely distributed user cards and automated terminals.

Brief Summary Text - BSTX (8): The sophistication of card counterfeiting and credit fraud has increased with the widespread use of account and credit cards, and even greater security measures are currently needed to ensure the validity of card transactions. Conventional microprocessor cards employ resident programs to control access to data stored on the card, store a selected user PIN to confirm an authorized user, and prevent use of the card if an unauthorized user is detected, such as after a limited number of incorrect PIN entries. Although such microprocessor cards provide greater security than passive cards, the overall system is still vulnerable in that, once a valid user's PIN has been ascertained, a stolen card can be used for unauthorized transactions in any terminal, and the terminals themselves are subject to penetration. These vulnerabilities can be offset by limiting the authorized amount of the card, controlling access to the terminals, or requiring on-line confirmation of transactions. However, such measures again increase the cost of the system and decrease its utility.

Brief Summary Text - BSTX (9): One potential area of application of automated systems employing account or credit cards is in postage vending and metering machines. Purchases of postage and mailing transactions are made primarily in person with cash through tellers at post offices. Only limited types of postage stamps can be purchased from public vending machines. Most private postage metering machines have limited operational features and must have their metering devices removed periodically

to a post office for refilling. The size and weight of the metering devices make them inconvenient to carry. Some metering systems can be refilled by a remote computer, but the caller must still phone the computer center and execute the operator's instructions on the postage meter manually.

Brief Summary Text - BSTX (10): The elimination of cash purchases, in-person mailing transactions, unnecessary limitations on automated postal services, and physical refilling of postage metering machines could greatly reduce the waiting lines at post offices and facilitate the wider dissemination of postage vending and metering machines for the convenience of users and provide greater access to postal services. The use of account or credit cards for automated postal machines has been considered. However, the security problems of conventional card automated systems would require that used cards be validated only for relatively small amounts of prepaid postage, that vending and metering machines provide limited postal products and be refilled with limited total postage amounts, and that access to the machines be strictly controlled. These restrictions are a substantial obstacle which contribute to the difficulty of implementing an automated postal transaction system.

Brief Summary Text - BSTX (12): In view of the foregoing disadvantages and problems of conventional systems, it is a primary purpose of the invention to provide an automated transaction system which has security features that will facilitate the widespread use of account or credit cards for off-line transactions and the dissemination of automated transaction terminals to which access does not have to be strictly controlled. A principal object of the invention is to provide an interactive card/terminal system in which the card and the terminal each have a security feature which prevents the completion of a requested transaction unless a secure handshake recognition procedure is mutually executed between the card and the terminal such that they each recognize the other as authorized to execute a transaction. In particular, it is desired that the card and the terminal cooperate together to execute a simultaneous dispensing of value by the terminal and debiting of an authorized balance by the card.

Brief Summary Text - BSTX (15): A particular embodiment of the invention is a mutual handshake recognition procedure executed as follows: (1) upon confirming that a requested transaction is authorized, the card passes to the terminal a word comprising a randomly generated or other object number encrypted by a first resident algorithm and a key number stored in the card; (2) the terminal decodes the number using a corresponding inverse of the first algorithm and the key number; (3) the terminal sends back to the card a second word comprising the decoded random number encrypted by a second resident algorithm and the key number; (4) the card decodes the second word using a corresponding inverse of the second algorithm and the key number and compares the decoded number to the one originally sent; (5) if the numbers match, the card microprocessor debits its authorized balance for the indicated amount of the transaction and sends an actuation signal to the terminal to proceed with the transaction; and (6) upon receipt of the actuation signal, the dispensing microprocessor actuates the

dispensing section to complete the transaction. The transmitted actuation signal may also be encrypted and decoded by the above algorithms or a similar method.

Brief Summary Text - BSTX (20): The postage metering terminals according to the invention are also provided with means for allowing a post office or carrier to authenticate the postage marks or waybills that are printed. In one embodiment, the terminal printer prints within or under the postmark a coded number or sequence of marks corresponding to an element of the postmark, such as the amount of postage, the terminal identification number, and/or the sender's zip code. The marks may be disguised or made invisible by printing with a magnetically or optically readable ink to deter tampering or unauthorized simulation. They may then be machine-read by the post office or private carrier company to determine whether the printed postmark was printed by an authorized printer, and at the same time provide an audit trail to the sender.

Detailed Description Text - DETX (4): When conventional microprocessor cards are issued to individual users, a validation procedure is executed on a validating terminal. The procedure generally requires the issuer to enter the correct manufacturers' serial number of the card in order to confirm that the card is authorized. A PIN is then assigned to or selected by the cardholder and stored in the secret zone. Moreover, a secret key number unique to the issuer, which may be common to a class or chronological series of cardholders, may also be stored in the secret zone. In some card systems, the secret key is used as an argument of an encryption algorithm to send an encrypted word to the terminal for verification. If the word can be decoded by the terminal to derive the secret key, the card is presumed to be authentic. Upon completion of the validation procedure, the card MPU irreversibly alters its program so that no further words can be written in the secret memory zone. Thereafter, upon using the card, a user must enter the correct PIN in order to confirm that the card is being used by its authorized user. Conventional microprocessor cards also have the feature of temporarily or permanently locking the card from use if a succession of incorrect PIN entries on a terminal is detected.

Detailed Description Text - DETX (9): The card MPU 60 executes an internally stored (firmware) program to check whether a requested transaction is authorized and, prior to debiting the card account balance, to perform a secure handshake recognition procedure (described further below) with a microprocessor in the terminal. Although the handshake procedure can be performed with an operations microprocessor for the terminal, or one remote to the terminal, it is preferred in the invention that the procedure be performed with a secure microprocessor embedded in the actual value dispensing section of the terminal. The value dispensing section is a separate element in the terminal, and its microprocessor is made physically secure, such as by embedding it in epoxy, so that any attempt to tamper with it would result in rendering the value dispensing section inoperative. For the postal transaction terminal of the invention, the microprocessor is embedded in the printer unit which prints the postmark.

Detailed Description Text - DETX (14): The interactive operation of the card/terminal system will now be described. Upon inserting a card in slot 11, the trip switch 22a is triggered, and the terminal MPU 30 initiates an identification request procedure to confirm that the card is being used by an authorized user. For example, the terminal MPU may cause a prompt to appear on the display 32 requesting that the user enter a PIN. The number entered by the user is sent by the terminal MPU to the card MPU where it is checked against the PIN number(s) stored in the secret zone of the card's memory. If the number matches, the card MPU notifies the terminal MPU 30 to proceed. If the card is restricted for use only in particular machines, the card may request the terminal's MIN and check it against a stored list of authorized terminal numbers. If the terminal is restricted for use only with certain cards, the terminal may check the PIN or a card identification or account number against a stored list of authorized card numbers. As another security feature, the card program may check the number of incorrect PIN entries attempted or a card expiration date written in memory at the time of issuance. If the incorrect PIN entries exceeds a predetermined number, or if the current date indicated from the terminal MPU 30 is past the expiration date, the card MPU 60 can lock the card against further use until the user has had it revalidated by the issuer.

Detailed Description Text - DETX (17): A basic principle of the invention is that the actual execution of a value-exchanging transaction is securely controlled by a mutual handshake recognition procedure between a secure microprocessor maintaining the card account balance and a secure microprocessor controlling the value dispensing operation. The card's MPU must recognize the value dispensing section's microprocessor as valid, and vice versa, in order to execute a transaction. The card and the value dispensing section therefore can each remain autonomous and protected against counterfeiting or fraudulent use even if the security of the other has been breached. Since they are autonomous, the cards and terminals can be distributed widely with a low risk of breach of the system and without the need for strict access controls. It thus has significant cost and security advantages over conventional card automated transaction systems.

Detailed Description Text - DETX (24): At level I, the print head of the terminal is only operable to dispense value, i.e. print postage, if the encryption algorithms provided by the manufacturer match those of the card, thereby protecting against counterfeit cards and terminals. Even if the security of the manufacturer has been penetrated, and the encryption algorithms have been obtained by a counterfeiter, the secret key may be assigned at level II by the issuer and used in the handshake procedure, thereby deterring the use of counterfeit cards and terminals which do not have the secret key. At security level III, a card can only be used to operate a terminal if the correct PIN is known, and if initial confirmation procedures are passed. At security level IV, a card can only be used in a particular terminal identified by the correct MIN.

Detailed Description Text - DETX (51): If the user card is to be refilled, the user PIN is confirmed, and then the card is checked for any balance to be credited toward the

new amount or to the user's account. The old memory section is then locked from further transactions, and can only be used for reading out a transaction history. Upon a request for a new amount, either for a new card that has been validated or for a card to be refilled, the terminal MPU 30" opens a handshake channel, and the handshake procedure previously described is executed between the master MPU 162 and the supervisor MPU 172. When the handshake procedure is completed, the master balance is debited and the supervisor card proceeds to open a new transaction memory section in the user card into which the new balance is written. The program then provides at block 197 an end selection of further operations which may be carried out on the refilling terminal. For example, another refilling transaction may be processed, the supervisor card record may be updated, the newly validated user or master card may be embossed with a serial number or account number if the terminal is connected to an embossing machine, or operations may be terminated.

Detailed Description Text - DETX (52): The described refilling system is protected at several levels of security. First, a supervisor card is required, and the user card must be validated by the user PIN. The master card must be validated by the supervisor card and must execute the handshake procedure before the user card is credited with a new amount. The card/terminal system has the primary advantage that the debiting of the card balance is executed in the same time frame that the value dispensing operation is carried out, and the exchange can only be carried out for each transaction if the mutual handshake recognition procedure is executed between the secure microprocessors controlling each part. Also, the central issuer purchases the card/terminal system for the manufacturer with a given set of encryption algorithms, and then selects a unique secret key not known to the manufacturer. Thus, penetration of the manufacturer's security will not compromise the security of the issuer's system. By issuing cards with defined expiration dates or series numbers and changing the secret keys periodically, an issuer system can be made even more impenetrable to counterfeiters.

Detailed Description Text - DETX (53): The user's card is not merely a passive record of an account number and balance, but rather operates to affirmatively protect against unauthorized use of the card, for example, if a succession of incorrect PIN entries is made, if the card is used beyond its expiration date or in an unauthorized machine, or if a requested transaction is in excess of predetermined limits. Similarly, the value dispensing part of the terminal is protected against tampering by the physical bonding of the printer microprocessor to the print head.

Detailed Description Text - DETX (56): Further, the invention is not limited to the described automated postal terminals. The principles of the invention can be adapted to any other value exchanging transaction where it is desired to use an account card in an off-line automated terminal system. Thus, the described cards and value dispensing terminals can also be used for dispensing cash, printing tickets, issuing coupons, etc., and the user can possess a variety of cards each issued by a central issuer for the convenient purchase of different articles of value. Also, by implementing card and terminal MPU programs which check for authorized machine identification numbers

and card serial numbers, or execute the handshake procedure with different algorithms and/or secret keys, an issuer's system can be configured so that the issuer's cards and terminals may be made open or restricted to certain families, series or locations.

Detailed Description Text - DETX (57): The invention also encompasses other features which are useful adjuncts to the central concepts described above. For example, a transaction history printer may be provided from which a user can print a record of transactions stored in the card upon entry of the correct PIN. The various cards can be provided with notches on a border or coded key elements to prevent insertion of the wrong card in an incorrect terminal slot or in a terminal of another issuer system. Also, the invention can be adapted for on-line transaction systems. For example, the terminal MPU can be connected by a telephone line or local network to a central processing office for approval of a transaction prior to execution of the transaction. On-line confirmation may be desired for initialization and refilling transactions which are less frequent and of higher value than purchase transactions. As another security feature, the card or series of cards may be issued with encryption algorithms and/or secret key numbers which are changed periodically, and the encryption algorithms and secret keys corresponding to cards presented for a transaction can be loaded in the terminal at the time the terminal MPU establishes an on-line connection to the central office.